UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v. Case No. 13-CR-155

JEFFREY FELDMAN,

Defendant.

MOTION TO DESIGNATE THE CASE AS COMPLEX, MOTION FOR EXTENSION OF TIME TO FILE MOTIONS, AND MOTION FOR PRETRIAL SCHEDULING CONFERENCE

Jeffrey Feldman, by his attorneys Robin Shellow and Chris Donovan, hereby moves the Court for additional time to file motions in the above-captioned case, and further moves the Court, pursuant to Fed. Rule of Criminal Procedure 12(c) and 17.1, and 18 U.S.C. §3161(h)(7)(A), to vacate all previously scheduled motion, briefing and trial dates, to designate this case as complex, and to schedule a pretrial conference. As and for support for this motion, undersigned counsel shows to the Court as follows:

INTRODUCTION AND HISTORY

This case began with the Government obtaining a search warrant for Jeffrey Feldman's dwelling and his computers. Among the items seized were a desktop computer, various external drives, and papers that appear to indicate Feldman resided at the residence (phone bills, mail, etc...). Amongst the documents seized were a handful of pages with what appear to be handwriting relating to passwords. One password mentioned pages appeared to be connected to a Time Warner Cable account. Another

password connected page is titled "Computer Use Instructions" and contains the specific computer password for the computer seized. (Exhibit 1). Approximately three months later, the Government filed an *Ex Parte* Application under the All Writs Act on April 3, 2013 in Case No. 13-mj-449 seeking to compel Mr. Feldman to decrypt various drives despite having seized a document in the search that appears to have been a password for a multi-terabyte drive that, according to the Government, contains thousands of images of child pornography.[i]

Feldman, (then known as "Interested Party"), in his original request to stay the compelled decryption, articulated that there appeared to be probable cause problems as the Government's probable cause seemed to be based on non-single source downloads -- i.e. that the Government could not identify with particularity from whose computer the pornography observed by the agent had been shared. (Doc. 7-1, ¶14A)[1]. Feldman's attorney was not the only person to identify the problem.[2] The Government alleges that

[1] In the world of Peer to Peer (P2P) Networks, when a file is requested to be downloaded, it can be, and many times is, downloaded from multiple sources (computers) in different locations and then reassembled at the client end. This is possible by identifying exactly the same file at different locations using the Sha1 values. This process of downloading pieces from different locations was developed in order to help balance the load on a particular P2P network. In the case of a P2P sting it is desirable to do a "Single Source Download" where the entire file is downloaded from the single target computer because it is possible that the target computer just has the file name and knowledge of what computer the file is on but not the file itself. The "enhanced" P2P software used by OCE 4583 was designed to specifically perform these single source downloads but, apparently, was only able to acquire the Sha1 hash values of the files and or downloads from multiple sources. (Doc. 1, pg. 5, ¶ 12)(Doc. 7-1, 4:14A)

[2] Special Agent Ungerer working with SA Banner In the Matter of the Search of 120 Kilps Court West, Waukesha, WI , Case No.: 13-M-472, ¶12, page 5: Files being shared by P2P clients are processed by the client software. As part of this processing, a hashed algorithm value (i.e. MD5, SHA-1, and eD2K MD4) is computed for each filed being shared, which uniquely identifies it on the network. A file processed by this hash algorithm operation results in the creation of an associated hash value often referred to as a digital signature. Some hash algorithms provide a certainty exceeding 99.99 percent that two or more files with the same hash value are identical copies of the same file regardless of their file names. The slightest alteration of any file will result in a completely different hash value. By using a hash algorithm to uniquely identify files on

Feldman utilized a file sharing program called eMule. Feldman also averred that one of the many reasons for his refusal to decrypt was that he did not want to provide information that would subsequently be used to save the original warrant should the original warrant be found to lack probable cause. (Doc. 7, p.5-7)

On August 27th and 29th the Government turned over to defense counsel 5 CDs of discovery containing approximately 73 pages of actual reports and other documents. (photos taken during execution of search warrant at residence and items seized at residence, employment records, phone records, credit card statements, Best Buy purchases and Time Warner Cable documents). Despite the numerous documents, the Government has disclosed only a single 21 page computer forensic summary report despite previous sworn statements that the Government and its Computer Analysis Response Team (CART) spent months attempting to decrypt the seized drives that they assert contain as many files as the Library of Congress—all the while having seized the type written "Computer Use Instructions" (SW_000088) giving them complete access to his internet cache. (Exhibit 1).

Of note, little to nothing in the discovery received to date demonstrates that the Government has anything more than file names of alleged child pornography pictures retrieved from the temporary internet folder on the seized desktop computer that

---

a P2P network, the network efficiency is greatly improved. Because of this, typically, users may download a selected file from numerous sources by accepting different segments of the same file from each source and then reassembling the complete file on the local computer. This is referred to as multiple-source downloads. The client program succeeds in reassembling the file from different sources only if all the segments came from the exact copies of the same file. P2P file sharing networks use hash values to ensure exact copies of the same file are used during this process.

contained 1,009 file names, as described in the original All Writs filing.[3] In order to figure out why the Government has engaged in such a complex game of cat and mouse, counsel for Feldman has several hypotheses which cannot be ruled out without extensive discovery litigation.

Hypothesis No. 1

The titles found on Feldman's desktop drive didn't originate from the user, but could have come from the internet without the user's knowledge or permission thus explaining why the 1,009 titles may have no evidence (i.e. actual pictures or videos) to support those titles.

Hypothesis No. 2

Those titles could have already been present in the eMule program when the user downloaded it. A search of the eMule program that is done utilizing only the word "new" returns in nanoseconds many titles that sound exactly like every other title encountered in this and other child pornography cases and were listed on the screen. Of note, also appearing on the screen were search terms that SA Banner and other special agents in this and other cases allege to be the search terms associated with those seeking child pornography. (Exhibit 2).

[3] The Complaint and the Indictment both contain references to names of files found in the temporary internet folder as well as other names. It is important for all of the names contained in the temporary internet folder and their corresponding SHA values and hash values be disclosed and compared against the files in the computer of the undercover agent so as to be able to determine whether the file names originated with the undercover agent.

Hypothesis No. 3

EMule or its mega parent eDonkey, Kad is not a decentralized file sharing program and maintains a file sharing server that stores, at the very least, the names and searches of the files its users share. Thus, every person who downloads the eMule program who searches for the word "new" will receive searches and titles sufficient for neutral and detached magistrates to find that there is probable cause to search the dwelling upon which an IP address is connected to.

Hypothesis No. 4

The FBI has recently adopted a novel investigative technique: posting hyperlinks on file sharing programs that purport to be illegal videos of minors having sex, and then raiding the homes of anyone willing to click on them. Undercover FBI agents used this hyperlink-enticement technique, which directed Internet users to a clandestine government server, to stage armed raids of homes in Pennsylvania, New York, and Nevada last year. The supposed video files actually were gibberish and contained no illegal images. Regardless, anyone who clicks on a FBI link that contains no child pornography could be automatically subject to a dawn raid by the federal and state police that comprise the Internet Crimes Against Children (ICAC) task forces.[4] This hypothesis appears to have some bearing on Franks-type suppression issues as page 10 of 15 of the

[4] It is likely that the length and description of the contents of the two movie files in the Application for the initial search warrant referenced in ¶10, were obtained by OCE 4583 or NCMEC when retrieving copies of the files from their own databases using the Sha1 values and viewing the length and content of the copies, or downloading the files in a non-Single Source Download. (Doc. 7-1, 5,¶14(D), 13-mj-449)

only forensic report received indicates that found on QMW2: were "Three (3) video files possessed MD5 (Messenger Digest algorithm 5) hashes which match those from the UC (under cover) session."

Hypothesis No. 5

A new virus discovered by McAfee's virus reporting site that seems to be planting and distributing suspected child pornography files and is being used by the ICAC task force to conduct raids, searches and seizures, all data taken including irreplaceable family photos and videos. Magistrate Callahan in Doc. 6, 13-mj-449-WEC, decided to reverse his original decision denying the Government's request for compelled decryption based on the Government's then-new disclosure that personal pictures of Feldman were obtained during the 10 weeks it had previously spent decrypting storage media for which it had the password. *Id.*

This new virus has three rogue programs: Ares.exe, Shareaza.exe, and emule.exe. *According to CNET the virus has been classified as the Win32/MoliVampire. The file is what many suspected as a trojan, size 10067968 B, and reveals a lot of details of this virus. The virus has different codenames and different file sizes so these viruses are all different in variants and threat level.*

The following constitutes a non-exhaustive list of discovery requests that need to be ruled upon by the Court should the Government not agree to produce each item:

1. All digital or paper reports as to what the undercover law enforcement officer did leading up to search (online investigation). (Doc. 1, p. 7, Case No. 13-MJ-421).

2. Any reports on "rancho torpedo" and "kleuterkutje" on the ICAC website that is used by law enforcement to locate individuals who distribute child pornography. (Doc. 1-1, ¶ 27(e), 13-MJ-449).

3. Any and all keyword searches ran on ICAC related to Case Nos. 13-MJ-421, 13-MJ-449, and 13-CR-155.

4. All reports attempting to break encryption for ten weeks to locate files referenced in Search Warrant, Complaint, Indictment, or All Writs Act filings. (Doc. 1, p. 4; Doc. 1-1, ¶ 20(a), 13-MJ-449). [5]

5. Forensic copies of hard drives that do not contain the alleged contraband as well as an opportunity for experts to examine the original hard drives.

6. Forensic examination reports referenced on discovery page number R_71 (CART Report) of all drives examined.

7. FBI 302 report's referring to all of the above.

---

[5] Forensic analysis of the remaining 9 storage devices show that they contain data but that the data is encrypted (b,c,e,i,j,m,n,o,p)… Agents recovered other passwords that have been used by Feldman. These passwords tend to be some combination of letters from his first and last names and arbitrary number values. The use of the letters and numbers make it difficult for law enforcement to crack the encryption. Law enforcement has already spent a great deal of time and resources attempting to recover the files and information as directed by the Court. Agents assigned to the FBI-Milwaukee Computer Analysis Response Team (CART) have spent over 10 weeks working on decrypting Feldman's storage devices. Their efforts thus far have been unsuccessful. (Doc. 1-1, 4,¶¶15, 16, and 20(a))

Additionally, FBI-Milwaukee enlisted the assistance of the FBI's Cryptological and Electronic Analysis Unit in an effort to decrypt Feldman's storage Devices. Despite working of decrypting Feldman's storage devices for approximately 8 weeks, their efforts have also been unsuccessful. (Doc. 1-1, ¶20(b)).

8. Examination of the computer utilized by the agents prior to executing the warrant at the Feldman residence.

9. Guidelines/Protocol of FBI and ICAC investigation of Peer to Peer (P2P) networks, including those related to investigations of individuals suspected of possessing or distributing child pornography.

10. Hash values for all pictures on ICAC website/library of pictures related to child pornography on eMule.

11. Hash values for all files represented as child pornography by agents, when in reality those files may not have been child pornography and were used as a ruse by agents.

12. Identification of any and all virus-like links used to conduct raids, searches, etc…, including Win32/MoliVampire.

13. Validation studies for any computer forensic program utilized in this case -- none of which the manufacturer will provide to anyone other than the Government.

14. Any computer forensic report, EnCase report, FTK, or any other program agents used to analyze the drive. (See Exhibit 3).

15. Any other IP addresses for multiple-source downloads associated with this investigation.

16. File names for all hash values and SHA-1 values reported in any documents related to Doc. 1, 13-MJ-421 and this case.

17. Any technologies utilized including computer-assisted scans to determine if computer evidence described by the warrant contained only file names and not images.

18. Any materials showing communications via phone or email between Attorney Shellow, Mr. Feldman and/or Attorney Donovan.

19. Any Title III materials, including applications for warrants, related to this case.

20. All MD5s (Message Digest algorithm 5) utilized in Under Cover investigations involving eMule.

Until these materials are either produced by the government, or ruled on by the Court if contested by the government, Mr. Feldman cannot know what substantive motions he should bring to challenge the evidence in this case. In short, this case is complex and extended due to the amount of discovery materials that have not yet been produced by the government but that Mr. Feldman believes must be, and due to the motions that must be litigated both regarding discovery and regarding substantive legal issues pertaining to the manner in which the evidence in this case was obtained.

WHEREFORE Feldman respectfully move the Court for an order vacating all previously scheduled briefing and trial dates in this case and for the setting of a scheduling conference pursuant to Fed. Rule of Criminal Procedure 12(c) and 17.1, and to toll all applicable time limits pursuant to 18 U.S.C. §3161(h)(7)(A). Mr. Feldman hereby waives his statutory right to a Speedy Trial under the Speedy Trial Act so as to have time to properly investigate this case, review all discovery, and raise all substantive motions challenging the evidence in this case.

Dated at Milwaukee, Wisconsin on this 3rd day of September, 2013.

Respectfully submitted,

s/ Robin Shellow
Robin Shellow, # 1006052
THE SHELLOW GROUP
324 West Vine Street
Milwaukee, Wisconsin 53212
Tel: (414) 263-4488
Fax: (414) 263-4432

Christopher Donovan, #
PRUHS & DONOVAN, S.C.
757 North Broadway – 4th Floor
Milwaukee, Wisconsin 53202
Tel: (414) 221-1950
Fax: (414) 221-1959

Attorneys for Jeffrey Feldman – Defendant

[i] **Case No. 13-mj-421-WEC-1 (Search Warrant Matter)**

January 22, 2013 a search warrant was issued to search the premises of 2051 S. 102nd St., Apt. E, West Allis, WI. (Doc. 1)
January 24, 2013 the Search warrant was executed. (Doc. 2)

Case No.: 13-mj-449-RTR-1 (Decryption Matter)

April 3, 2013 the Government filed an Application Under the All Writs Act to compel the decryption of Feldman's computers that were seized from his home on January 24, 2013 pursuant to a search warrant. (Doc. 1)
April 19, 2013 Magistrate Callahan, Jr. entered an Order denying the Application to Compel Decryption. (Doc. 3)
May 8, 2013 undersigned counsel learned of the All Writs Application and filed her Notice of Appearance on behalf of interested party Jeffrey Feldman. (Doc. 4)
May 16, 2013 Government files a Request for Reconsideration of the United States Application under the All Writs Act. (Doc. 5)
May 21, 2013 Magistrate Callahan, Jr. entered an Order granting Government's *Ex Parte* request for reconsideration of the United States Application under the All Writs Act. (Doc. 6)
May 31, 2013 Interested Party Feldman files Objections as to the Decryption of the Seized data storage system. (Doc. 7)
June 3, 2013 Interested Party Feldman files an Emergency Motion to Vacate the May 21, 2013 Order or in the alternative to Stay the May 21, 2013 Order. (Doc. 8).
June 4, 2013 Judge Randa entered an Order granting the Motion to Stay. (Doc. 9)

June 28, 2013 Government files a Motion to Produce / Provide the Court with decrypted contents of encrypted digital media, Ex parte and under Seal. (Doc. 10).
July 2, 2013 Interested Party Feldman files a Motion to Quash Government's Motion. (Doc. 12)
July 16, 2013 Brief in Opposition by Feldman as to Decryption of a Seized Data Storage System. (Doc. 14)
August 14, 2013 Government files a Motion to Stay the Briefing schedule (Doc. 22) and Amended motion to stay the briefing schedule. (Doc. 23)
August 14, 2013 Interested Party Feldman filed his response to the Government's Amended Motion to Stay the Briefing Schedule. (Doc. 24)
August 16, 2013 Judge Randa entered an Order Denying the Government's Motion to Stay the Briefing Schedule. (Doc. 25)
August 16, 2013 Government files a Motion to Dismiss the Application to Compel Decryption. (Doc. 26.)

Case No. 13-CR-155-LA-AEG-1

August 13, 2013 Complaint is signed by Magistrate Nancy Joseph, Feldman is arrested at work and appears for Initial appearance at 3:00 p.m. (See Doc. 1 and 2)
August 14, 2013 Pretrial Services Report-Bond Study is Filed and Order for Temporary Detention is Ordered. (See Doc. 3 and 4)
August 15, 2013 Bond Hearing is held before Magistrate Nancy Joseph. (Doc. 5)
August 20, 2013 Indictment is filed. (Doc. 6)
August 26, 2013 Feldman is Arraigned. (Doc. 9)
August 26, 2013 Pretrial Order is issued. (Doc. 10)
August 26, 2013 Feldman posts bond and is released from custody. (Doc. 11).